CHAPTER 7
OTHER HAZARD ANALYSIS METHODOLOGIES

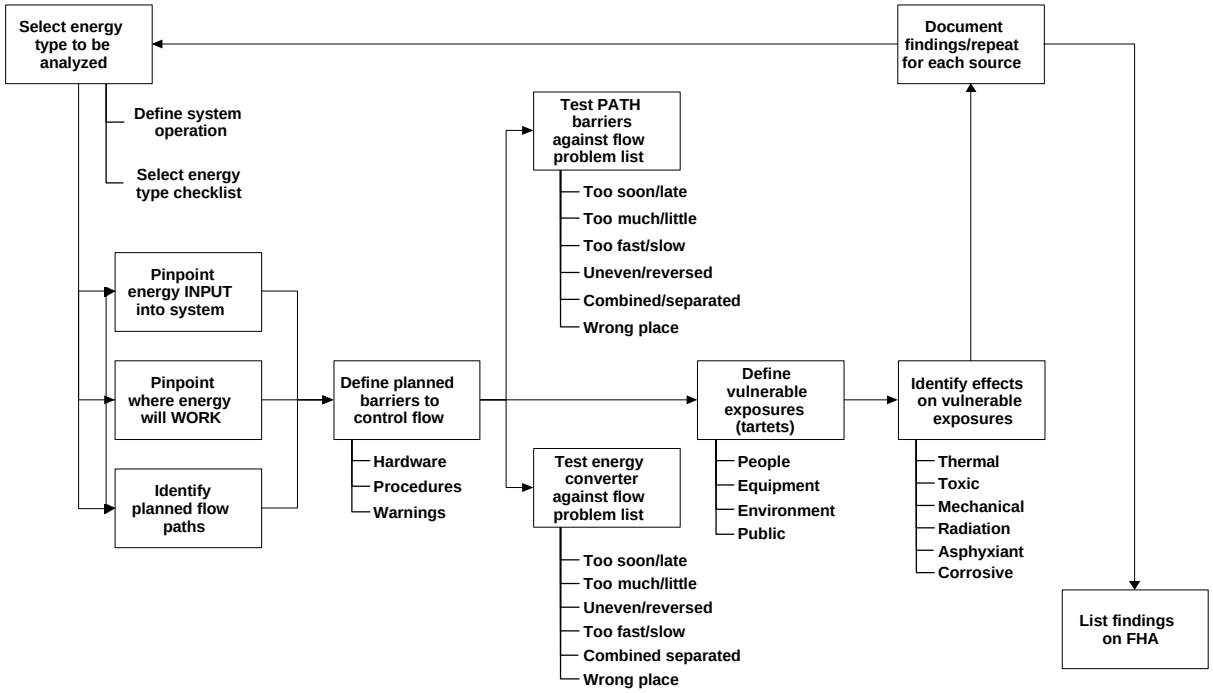
7.1 INTRODUCTION

Once initial system safety efforts are in progress, it may become necessary to do more in-depth analysis for the purpose of accurately assessing risk and controlling hazards. Eight of the more common in-depth risk analysis methodologies are described in the following paragraphs; any or all may be useful, depending on the facility and system life cycle phase, application, and operating environments.

7.2 ENERGY TRACE BARRIER ANALYSIS

7.2.1. Description. An Energy Trace Barrier Analysis (ETBA) is a qualitative analysis methodology used to develop more detailed knowledge of hazards. This technique shown in Figure 7-1 approaches the discovery of hazards by tracing the flows of energy into, through, and back out of a facility, system or operation. It is based upon the premises that:

- Mishaps arise from the risks within an operation.
- Mishaps interrupt or degrade the operation.
- Mishaps are an unwanted transfer of energy.
- The unwanted transfer of energy that produces injury to persons or property is due to a lack of barriers or controls over the energy.



Energy Trace Barrier Analysis Procedure
Figure 7-1

The ETBA process is particularly desirable and useful since it can be applied at any stage of the project to facilitate detailed analysis of those hazards discovered late in the project as well as those found at the beginning. The objective of ETBA is to find unsuspected hazards through methodical tracing of energy flows in the planned operation and across subsystem interfaces to locate potentially harmful diversions.

Each type of energy source, summarized in Table 7-1, should be considered individually from the perspective of the operations components and whatever subsystem energy control strategy may exist. The operation needs to be analyzed at the input/use/output level for each energy type to determine if the operation's plan or design addresses realistic potential control problems and satisfactorily controls them.

ETBA is used when concern over possible unacceptable loss indicates a need for better understanding of the operation. This is particularly true when lethal or significantly destructive energy flows characterize the operation and experience with the change or operation does not exist, or there has been a high loss rate, or behavior of certain energy interfaces is not known. ETBA is feasible because it is easy to identify the energy sources in almost any circumstance; the drawback is that performing an ETBA requires detailed familiarity with the operation or system. ETBA requires the services of someone who intimately understands the operation and can trace energies and barriers/controls thoroughly.

The ETBA is performed by tracing the sequence and logic of energy flow through the operation. For each energy type, the flow must be tracked to each transfer or use point, and each physical or procedural barrier to the energy must be considered to determine what harmful outcomes are likely to occur when:

- Too much or too little energy flows;
- The energy flows too soon, too late, or not at all;
- The energy flow is blocked or impeded in its pathway;
- The energy flow conflicts with another energy flow at a transfer or use point; and
- A barrier degrades, is disturbed, or does not function at all.

For a mishap to occur there must be an energy source with a release flow of energy to a target in the absence of adequate barriers. The flow or transfer of energy is the path between the energy source and the target or component of the operation being protected.

Table 7-1
Energy Types and Examples for Energy Traces
Caused by Internal Events:

1. Electrical
   - ac/dc flows
   - stored electric energy
   - electromagnetic radiation
   - static charges/flows

2. Mass/Gravity/Height
   - falls and drops
   - falling objects
   - falling hazardous materials

3. Rotational Kinetic
   - machinery
   - fans

4. Pressure/Volume & Kinetic Displacement
   - container ruptures and explosions
   - vacuum creation
   - liquids spill/flood
   - vapor expansion

5. Linear Kinetic
   - projectiles
   - rams, moving parts
   - shear press
   - vehicular movements, prints, pre-stressed members

6. Chemical Reactions
   - corrosion, oxidation, combustion, or
   - interactions among deposited materials,
   - polymerization,
   - decomposition,
   - toxic asphyxiant, anesthetic

Table 7-1 (cont.)
Energy Types and Examples for Energy Traces

7. Thermal
   heat, cold
   alternate heat/cold
   radiation/conduction/
   convection, sublimation

8. Etiologic
   viral,
   bacterial,
   fungal

9. Ionizing radiation
   gamma,
   alpha,
   beta

10. Noise and Vibration

11. Human Interactions

Caused By External Environmental Events:

1. Terrestrial
   earthquake, flood, landslide
   subsidence, compaction, cave-ins, water table

Caused By External Events

1. Radiation, explosions, projectiles,
   noise, vibration, fire

2. Atmospheric
   wind, rain, snow, lightning,
   hail, and acid rain

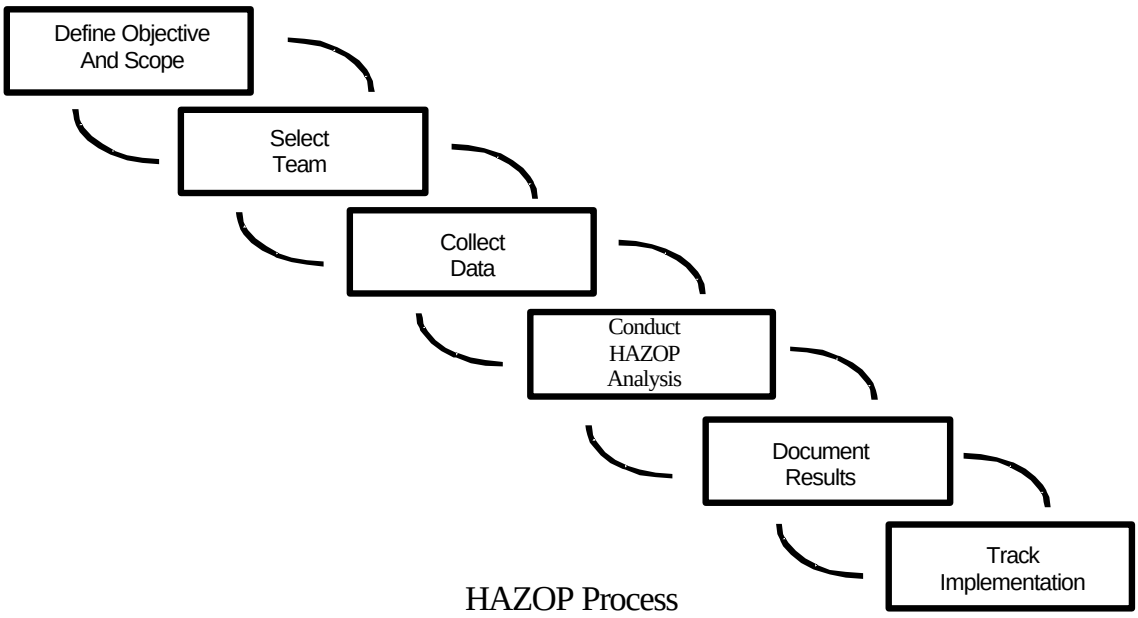
7.2.2. Results. In performing ETBA, an engineer develops and maintains a listing of energy sources and the hazards associated with each energy form source. Identified hazards are included in the Facility Hazard Analysis (FHA), or the Hazard Analysis Tracking Index (HATI) if the FHA is complete.

7.3 HAZARD AND OPERABILITY STUDY

7.3.1. Description. The Hazard and Operability (HAZOP) Study is a qualitative method of analysis used in identifying risk related to highly hazardous substances. The method provides a means of identifying a multitude of process hazards. It is used to identify potential hazards and operability problems early in the acquisition cycle at the time of design development of a process. Since the method can be applied early, the potential cost needed to eliminate or correct the hazard is minimized. The HAZOP is performed by an interdisciplinary team of experts who systematically examine each part of a process. This team identifies how deviations from the design intent can occur and whether the collective or individual deviations can create hazards.

The HAZOP is a structured group analysis technique for stimulating one's imagination in order to identify and assess the significance of all the ways a process unit can malfunction or be improperly operated. Its purpose is to identify potential process hazards due to system interactions or exceptional operating conditions.

The analysis objectives are to identify deviations from the design intent of the system. Then the analyst determines the safety concerns associated with the identified deviations. Finally, recommendations are proposed for resolving safety concerns or accepting risk. The HAZOP process is shown in Figure 7-2 below.



HAZOP Process
Figure 7-2

An optimum team should range in size from four to eight members and include designers, operators, and users.

The first step in a HAZOP is to identify the "node" to be analyzed. Some of the key items used in selecting nodes are:

- The next design change placed on the system,
- When a significant change of state occurs,
- Separate equipment items, and
- Different processes

Once a node has been selected, it is analyzed with respect to guide words with the process conditions. Guide words (no, more, less, reverse, etc.) are coupled with process conditions (flow, pressure, temperature, etc.). Table 7-2 offers a simplified application.

Table 7-2 - Guide/Process Condition

GUIDE WORD	**PROCESS CONDITION**
No	Flow
More (High, Long)	Pressure
Less (Low, Short)	Temperature
As Well As	Level
Part of	Time
Reverse	Composition
Other Than	pH

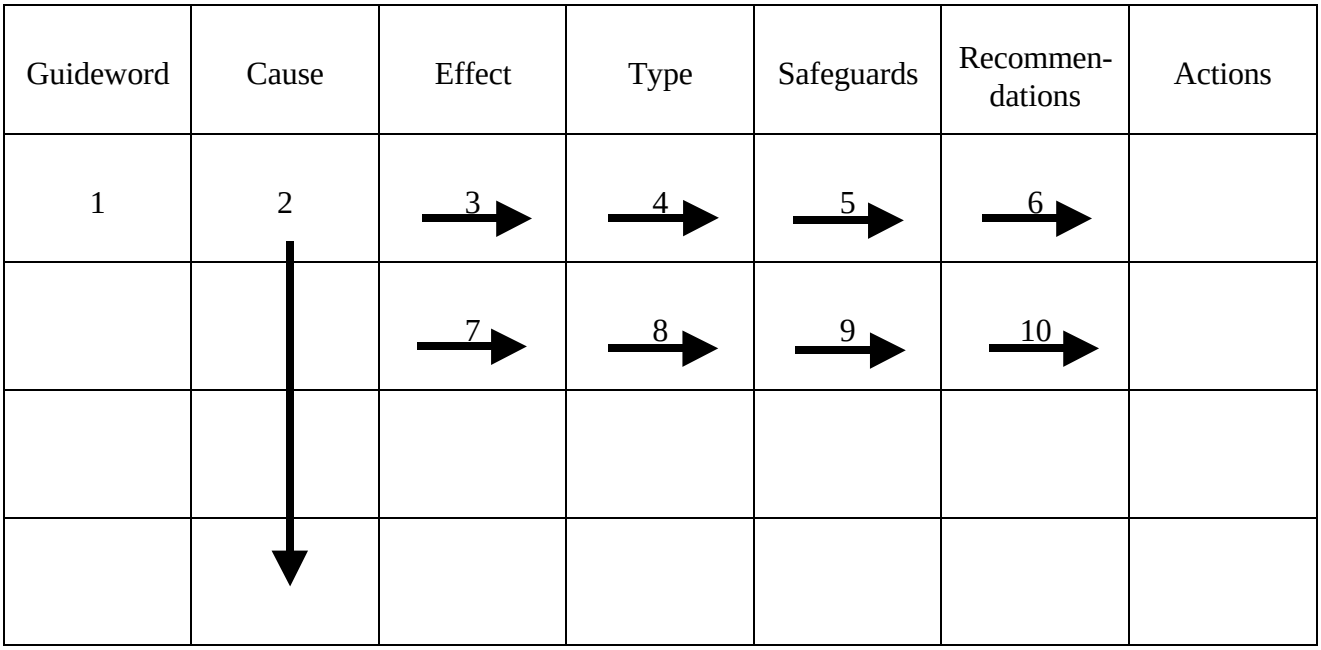
Guide Word plus Process Condition = Deviation

When organizing a HAZOP team one should consider the members' experience and background. Once a guide word is combined with each process condition the team brainstorms the possible deviations leading to bad consequences. One example is high pressure leads to:

- Death, personnel injury.
- Property damage.
- Environmental damage.
- Operational damage.

This determines the worst case credible effect on the node, taking into consideration single failure and ignoring safeguards already in place. This helps the analyst assess existing safeguards or propose additional safeguards if required.

7.3.2. Results. When the analysis phase is completed and all outstanding issues are resolved, the conclusions are prepared and a tabulation of recommended actions are prepared and submitted. Figure 7-3 shows a typical HAZOP worksheet. Sources of information typically include piping and hardware drawings, facility drawings, procedures, safety hazard analysis reports, and accident & investigation reports. The advantages of a HAZOP are that it is a very comprehensive hardware review, it is good for complex systems, and it provides very detailed results. The disadvantages of a HAZOP are that it is very time consuming, expensive, and may not pick up on multiple failures.



HAZOP Worksheet
Figure 7-3

The HAZOP is not a quantitative assessment and consequence probabilities are not normally part of the analysis unless other quantitative techniques such as fault trees are integrated into the overall effort; however, the results of the analysis are directly proportional to the extent that the HAZOP team understands the process and has defined all of the process elements. As stated earlier, HAZOP is only one method of hazard evaluation. Other methods may be more suited to a facility assessment depending on the needs of the project.

7.4 SUBSYSTEM HAZARD ANALYSIS

7.4.1. Description. The Subsystem Hazard Analysis (SSHA) is performed to identify design hazards in subsystems. For a facility, subsystems could include an industrial laser, a computer controlled fire detection and suppression system, a vacuum chamber or special purpose test equipment. The requirement for a SSHA is usually identified in the concept phase of a system or facility. Due to the complexity of the analysis, the analysis is usually specified in a procurement specification then completed by the equipment/subsystem manufacturer.

The analysis should find functional failures of subsystems that could result in accidental loss. Component and equipment failures or faults, and human errors that establish a hazard due to the functioning of the subsystem are analyzed. The analysis is completed by reviewing design drawings, engineering schematics, and specifications.

The SSHA should be completed no later than the beginning of system definition phase of the system life cycle. As the system and related subsystems are further defined during system definition and development, the analysis should be revised. A sample sheet from a SSHA completed for a signal system is provided as Figure 7-4 (Roland and Moriarty, 1990).

ANALYSIS TYPE:: SUBSYSTEM HAZARD ANALYSIS							
SYSTEM SIGNAL SYSTEM PREPARED BY _____							
SUB-SYSTEM POWER DATE _____ SHEET _____ OF _____							
ITEM NO.	COM-PONENT	FUNCTION	HAZARD DESCRIPTION	HAZARD EFFECTS	HAZARD CATEGORY & PROB.	RECOMMENDED CONTROL	RESOLU-TION
1	AUTO-MATIC TRANS-FER SWITCH	AUTOMATICALLY PROVIDES POWER FROM EITHER NORMAL OR EMERGENCY SOURCE	AUTOMATIC TRANSFER SWITCH WILL NOT SHIFT FROM POWER SOURCE TO EMERGENCY POWER WHEN POWER SOURCE IS LOST	SIGNAL FAILS	1D	PROVIDE "VITAL" SIGNALS TO SHIFT ALL SIGNALS TO RED (STOP) CONDITION WHEN NO POWER IS AVAILABLE	
2	AUTO-MATIC TRANS-FER SWITCH	AUTOMATICALLY PROVIDES POWER FROM EITHER NORMAL OR EMERGENCY SOURCE	NO POWER IS AVAILABLE FROM EITHER NORMAL OR EMERGENCY POWER SOURCE	SIGNAL FAILS	1E	PROVIDE BACK UP BATTERY POWER	

Completed Signal System SSHA Form
Figure 7-4

7.4.2. Results. The SSHA identifies hazards to personnel, equipment, facilities, and program resources caused by loss of function, energy sources, hardware failures, personnel actions or inactions, software deficiencies, interaction of components, inherent design characteristics, incompatible materials, and environmental conditions (within the subsystem).

Results of an SSHA are referred to the managing activity for inclusion in the hazard analysis documentation. Unresolved hazards are listed in the HATI.

7.5 SYSTEM HAZARD ANALYSIS

7.5.1 Description. The System Hazard Analysis (SHA) examines the interfaces between subsystems. In so doing, it must integrate the outputs of the SSHA. It should identify safety problem areas of the total system design including safety critical human errors, and assess total system risk. Emphasis is placed on examining the interactions of the subsystems. The SHA should examine subsystem relationships for:

- Compliance with safety criteria specified in subsystem requirements documents.
- Sets of hazardous events, independent or dependent to include failures of safety devices and common cause conditions or events that can result in system or facility hazards.
- Degradation of safety of the overall system or facility from normal operation of a subsystem.
- Software control functions that may adversely affect system risk due to software faults.
- Human control functions that may affect risk through human faults.
- The SHA begins during the early design phases. The SHA is updated when interfaces are defined and continues on through to the beginning of system operation.

7.5.2 Results. Results of the SHA are presented in tabular form. Identified hazards which are not resolved are included in the HATI. Figure 7-5 shows the results of a SHA for a tunnel pumping system.

7.6 OPERATING AND SUPPORT HAZARD ANALYSIS

7.6.1. Description. Most safety analyses are directed towards uncovering design problems associated with hardware. This is not the intent of an Operating and Support Hazard Analysis (O&SHA). The purpose of the O&SHA is to identify and evaluate the hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system/element. The O&SHA identifies, documents, and evaluates hazards resulting from the implementation of operations or tasks performed by persons and considers:

- The planned system configuration at each phase of activity,
- The facility interfaces,

ANALYSIS TYPE:: SYSTEM HAZARD ANALYSIS							
SYSTEM PUMPING SYSTEM PREPARED BY							
SUB-SYSTEM PUMP, CONTROLLER POWER DATE SHEET OF							
ITEM NO.	COM-PONENT	FUNCTION	HAZARD DESCRIPTION	HAZARD EFFECTS	HAZARD CATEGORY & PROB.	RECOMMENDED CONTROL	RESOLU-TION
1	POWER CABLE	TRANSFERS POWER BETWEEN SOURCE AND PUMP	PUMP CONTROLLER POWER CABLE FAILS - LACK OF POWER	LOSS OF PUMPING CAPABILITY - WATER FLOODS TUNNEL	1D	PROVIDE REDUNDANT POWER CABLE	
2	PUMP CON-TROLLER	PROVIDES CONTROL OF PUMP OPERATION	PUMP REMAINS ON CONTINUOUSLY - PUMP BURNS OUT	WATER FLOODS TUNNEL	1B	PROVIDE LOW WATER CUT-OFF FOR PUMP	

Completed Tunnel Pumping System SHA Form
Figure 7-5

- The planned environments, the support tools, or other equipment specified for use,
- Operation or task sequence,
- Concurrent task effects and limitations,
- Biotechnological factors,
- Regulatory or contractually specified personnel safety and health requirements, and
- The potential for unplanned events including hazards introduced by human error.

The O&SHA identifies the safety requirements (or alternatives) needed to eliminate identified hazards, or to reduce the associated risk to a level which is acceptable.

To perform an O&SHA, pertinent data such as procedures, sequence diagrams, operation and functional analyses, equipment layout diagrams, systems and subsystem design specifications, equipment and interface drawings, operations and maintenance instructions, and human factors engineering data should be obtained if available. A worksheet is commonly used to develop the hazards. It is similar to the FHA but with an operational event as the primary categorizing function. Operational events are sets of sequenced actions for operating, assembling, maintaining, repairing, calibrating, testing, transporting, handling, installing, or removing an assembly, component, or system. These events are generally documented in procedures. An analysis of the procedures is completed to ensure that:

- Required tasks, human-machine-environment and interpersonal relationships, and the sequences of operational steps will not lead to a mishap.
- Completing the procedure does not expose personnel to any hazards.
- Instructions are clear and effective and do not induce errors that could lead to mishaps.
- Alternative actions a person could take which could result in mishaps are precluded, or the effects of such actions are minimized.
- Safety-critical steps are highlighted with warnings and cautions.
- No extraordinary mental or physical demands are made for programmed operations.
- Times for accomplishment of safety-critical tasks are realistic.

The following should also be accomplished to ensure the procedures are safe:

- Examine the procedure and each step within the procedure for effect, necessity, and clarity. Personnel tend to take shortcuts in order to avoid arduous, lengthy, uncomfortable, or ambiguous procedures. The shortcuts can sometimes lead to errors and mishaps.
- Examine each procedure and each step, no matter how simple it appears, for possibilities of error, alternative actions, and adverse results.
- Determine whether or not special training, knowledge, or capability is required which the prospective operator might not have.
- Review the causes of error and attempt to eliminate or minimize the possibilities of as many of them as possible.
- Verify the proposed procedures by examining, demonstrating, and testing.

After the operating procedures are analyzed, the procedures should be verified. This verification should be done by persons not involved in writing or analyzing the procedures. A checklist should be used to assist in verifying the procedures. In addition, the analyst should try to perform the procedures as prescribed by the author of the procedures and then try to anticipate any alternative actions the user might take. The person performing the procedures should verify that safeguards will work as intended, that emergency stop systems can be reached and will stop an operation when they are supposed to, that detection and warning devices operate, that personnel protective equipment can be reached and donned within planned lengths of time, and that emergency routes and exits are practical.

7.6.2. Results. An O&SHA is very useful and can give valuable information, such as:

- Corrective or preventive measures that should be taken in order to minimize the possibilities of an error resulting in a mishap.

- Recommendations for changes or improvements in hardware or procedures in order to improve efficiency and safety.
- Development of warning and caution notes to be included in the most effective places in the procedures.
- Requirements for special information or training of personnel who will carry out the procedures.
- Recommendations for special equipment, such as personnel protective clothing or devices, which would be required for the operations to be undertaken.

Figure 7-6 shows the results of an O&SHA worksheet.

OPERATING & SUPPORT HAZARD ANALYSIS BATTERY BOX

STATION: Technician DATE: _____

OPERATIONAL MODE: Run SHEET NO: ____ OF ____

ID #	Process/Task	Hazardous Condition	Cause	Effect	Hazard Category	Hazard Probability	Status/ Recommendation
1.	Connecting/disconnecting emergency lights to sealed connections on battery box.	Water enters into connector	Connectors cracked or seal is defective.	Electrical shock to personnel.	1-Catastrophic	B- Possible	Daily inspection of connectors; Replace when deficiencies are detected.
2.	Removal and replacement of battery box.	Fall on personnel. Fall on equipment.	Lifting lugs fail. Nylon webbing fails.	Injury to personnel. Damage to equipment.	1-Catastrophic	B- Possible	A. Assure integrity of weld lugs. B. Perform regular inspections of webbing; Replace when frayed or worn. C. Train personnel in safe raising/lowering box. D. Train personnel to stand clear when box is being raised or lowered.

Example O&SHA Worksheet
Figure 7-6

7.7 FAULT TREE ANALYSIS

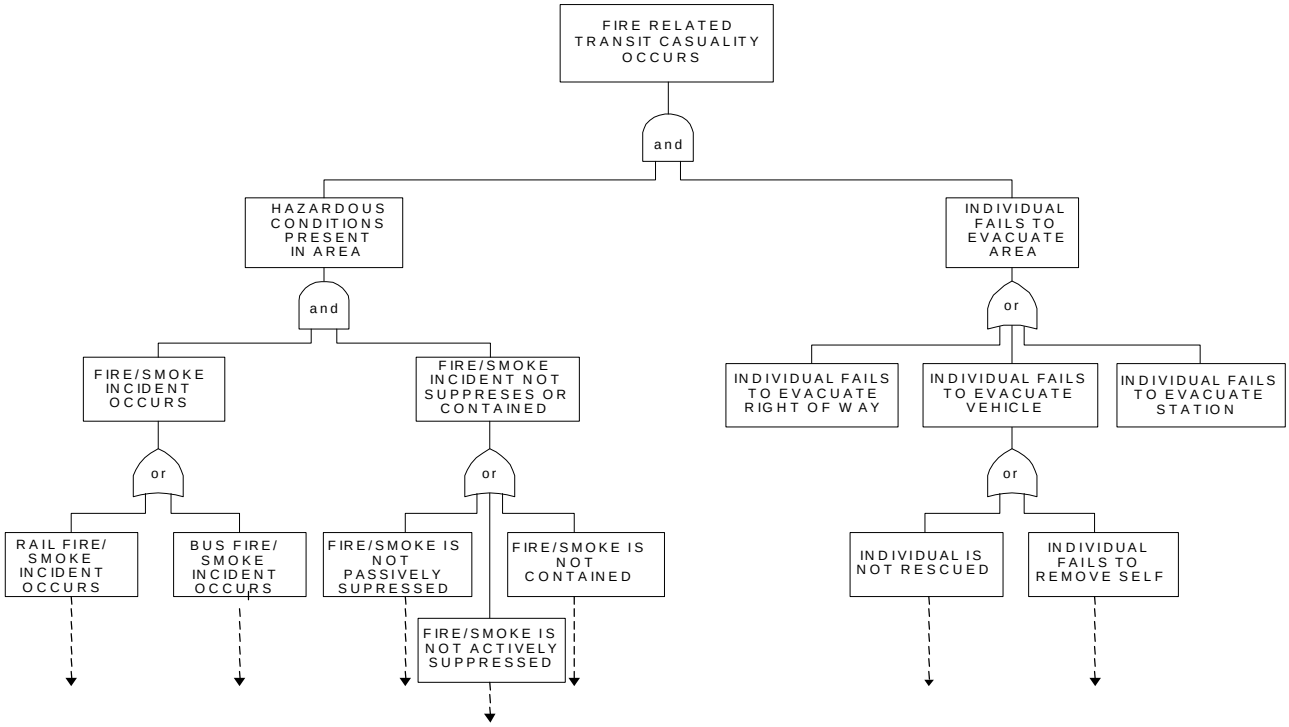
7.7.1. Description. A fault tree analysis (FTA) can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with

component hardware failures, human errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event which is the top event of the fault tree.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes of system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive, they cover only the most credible faults assessed by the analyst.

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively and often is. This qualitative aspect, of course, is true of virtually all varieties of system models. The fact that a fault tree is a particularly convenient model to quantify does not change the qualitative nature of the model itself.

A fault tree is a complex of entities known as "gates" which serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationship of events needed for the occurrence of a "higher" event which is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event. Thus, gates are somewhat analogous to switches in an electrical circuit or two valves in a piping layout. Figure 7-7 shows an example fault tree.



Example Fault Tree
Figure 7-7

7.7.2. Results The output of a FTA is a graphic functional failure representative of the system or facility. Though the FTA itself is qualitative, quantitative data can be annotated to the tree in the form of event or component failure probabilities, thus quantifying the FTA.

7.8 FAILURE MODE AND EFFECTS ANALYSIS

7.8.1. Description. The Failure Mode and Effects Analysis (FMEA) is a reliability analysis. The focus of the analysis is on single events or component failures that will cause a state of unreliability in the system (Roland and Moriarty, 1990). The objective of the FMEA is to view each identifiable component in the system in the context of two questions:

- How can the component fail?
- What will be the results of this failure downstream in the system or subsystem?

This effort can improve knowledge of potential component, subsystem, or system failures that were found by the FHA. The FMEA is used to methodically track each component's major failure effects into other subsystems and to develop an understanding of the hazardous impact on one component's failure on the rest of the system. As with the SSHA, this analysis methodology requires in-depth knowledge of the system, and is generally specified in a procurement specification and then completed by the system or equipment manufacturer.

FMEA analysis is conducted by asking each of the two above cited questions in relation to components and then projecting the likely physical and functional effects of the failures on other parts of the system. Effects of failure are stated in terms of associated damage or malfunction accompanied by qualitative assessments of frequency and severity suitable for Hazard Risk Indicator (HRI) ranking.

7.8.2. Results. The FMEA output is a columnar worksheet shown such as the one in Figure 7-8. An HRI code for each item may be substituted for the “Probability of Failure". One of the strengths of FMEA is that it promotes identification of problems associated with the interface of subsystems and/or components. Using the specified output format, detected hazards will be described for characteristics and recommended control action(s). Though the FMEA is qualitative, failure probabilities can be included for decision making purpose.

7.9 SOFTWARE HAZARD ANALYSIS

7.9.1. Description. The traditional approach to the hazard analysis of complex electromechanical systems is to treat electronic devices that process or originate system control signal as black boxes. This approach precludes analysis of the internal functioning of the box. Output reliability of the box is established relative to input and this value inserted into the system model as a quantitative representation of a pseudo-mechanical component of the system. When we replace the box with a small computer, processing instructions that have been permanently installed in the memory, we have quite another situation. If the software containing the

			FAILURE EFFECT ON			
COMPONENT NAME AND NUMBER	FUNCTION	FAILURE MODE AND CAUSE	NEXT HIGHER ASSEMBLY	END ITEM PRODUCT	PROBABILITY OF FAILURE (σ X 10^{-6})	CORRECTIVE ACTION AVAILABLE OR RECOMMENDED
Cover Cap	Keeps coffee from being thrown about: keep user from getting fingers into cap where they could be cut by rotor.	Plastic fractures and parts separate. Brittle plastic dropped on hard surfaces, stepped on, or subjected to excessive force when being put in place.	None	None	1	Select plastic which is not brittle.
Switch Activating arm (1)	User depresses and holds down free end in access hole to switch which operates mill.	Breaks off cap due to rough handling by user,. being stepped on, or dropped.	May cause cap to weaken and break if arm breaks off in cap.	May make product unusable.	100	Redesign. Put switch under cap, thereby eliminating area.
Case Case, plastic (1)	Major structural part which holds other assemblies together: protects against contact with moving and electrical parts.	Could be broken by impact or crushing.		Resultant sharp edges and points; may make it unusable.	0.5	Use impact resistant plastic.
Vibration dampers (2)	Brittle pads in case. Reduction of vibration and noise by separating metal motor frame from plastic case.	Deterioration of rubber. Could be lost since they are not glued in place.	Fatigue to brittle plastic.	Excessive vibration and noise.	0.01	Glue in place.

Example Failure Modes and Effects Analysis
Figure 7-8

instructions is error or fault free, then this component cannot fail and the statistical concept of measuring stochastic wearouts has no meaning. However, the software instructions may contain faults. This possibility will require an analysis of the computer program code that has become instructions to the hardware system (Roland and Moriarty, 1990).

Control systems and control computers are usually in a high state of flux. Both hardware and software need to be analyzed for all faults and failures, including using probabilistic risk assessment techniques. Because of potentially frequent changes, which are relatively easy to make compared to hardware changes, control systems and software need to be under strict change control, as per the Center configuration management plan. Software is coded by programmers working to a specification set forth by system designers. Software faults may take three forms.

- The so-called honest errors made by the programmer in coding the software specification. These are simple mistakes in the coding process that result in the software behaving in a manner other than that which the programmer intended.

- Faults due to incorrect software specifications or the programmer's interpretation of these specifications. These errors may result from system designer's lack of full understanding of system function or from the programmer's failure to fully comprehend the manner in which the software will be implemented or the instructions executed. In this type of fault the software statements are written as intended by the programmer.

- Faults due to hardware failure. Hardware failures may change software coding. Thus such software faults are secondary in that they originate outside the software.

A software hazard may be one of the following four types:

- An undesired signal causes an unwanted event in the system functional process.

- An undesired signal causes an out-of-sequence event.

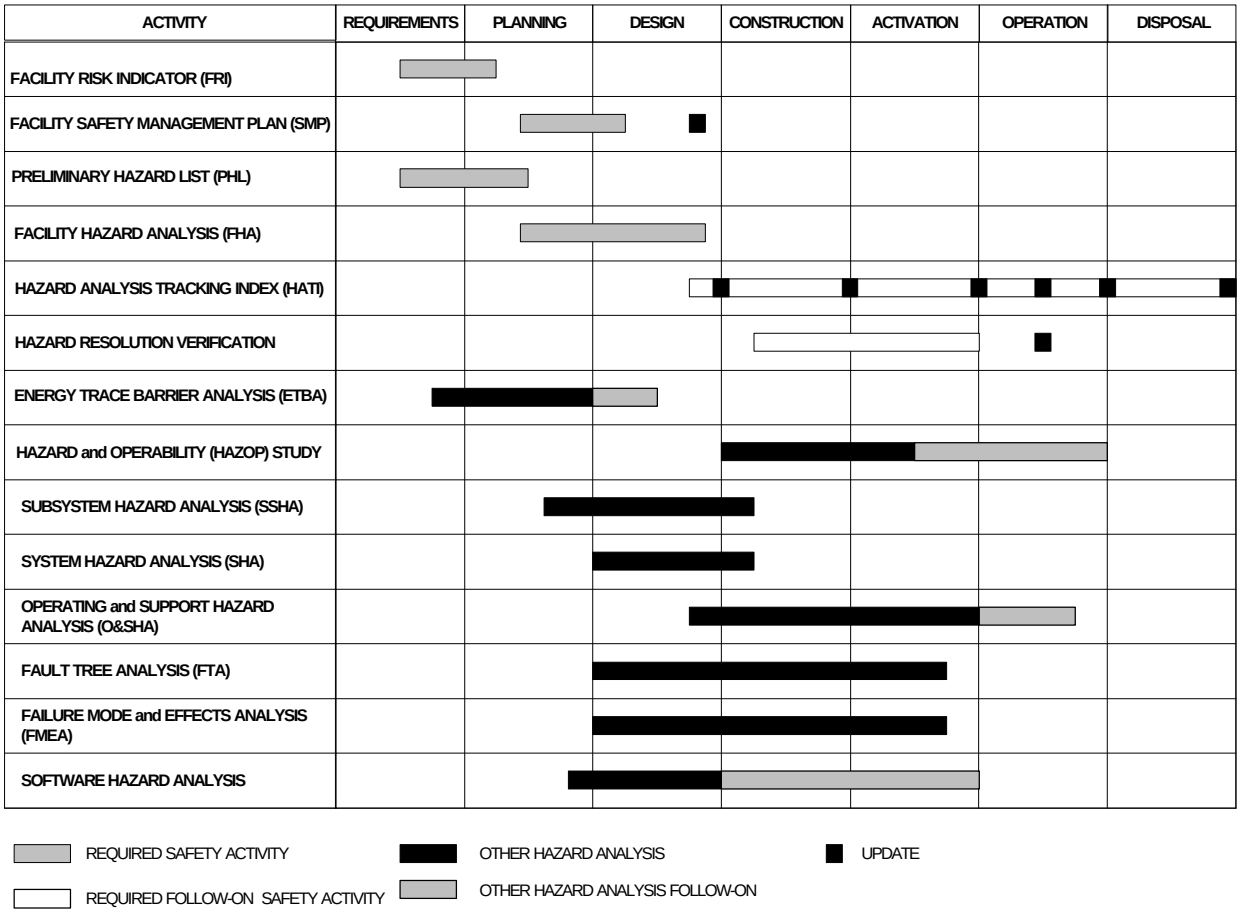
- An undesired signal prevents the occurrence of a needed event.

- An undesired signal causes an event that in magnitude or direction is out of tolerance.

7.9.2. Results. The results of the software analysis are as varied as the analyses themselves. Usually the data results are presented in tabular form. Graphs can also be used to depict causal relationships.

7.10 HAZARD ANALYSIS SCHEDULES

Figure 7-9 indicates the most appropriate time that the various hazard analyses can be performed throughout the facility life cycle. Obviously, many of them overlap during the facility life cycle.



Facility System Safety Milestone Activities
Figure 7-9

APPENDIX A
TYPICAL ENERGY SOURCES CHECKLIST

A. Acoustical Radiation

Equipment Noise
Ultrasonic Cleaners
Compressors

B. Corrosive

Acids
Caustics
Natural Chemicals (Soil, Air, Water)
Decontamination Solutions

C. Electrical

Battery Banks
Diesel Units
High Lines
Transformers
Wiring
Switchgear
Underground Wiring
Cable Runs
Service Outlets and Fittings
Pumps
Motors
Heaters
High Voltage Sources
Electrostatic Sources (low humidity)

D. Electromagnetic and Particulate Radiation

Radioactive Sources
Waste and Scrap
Contamination
Irradiated Experimental and Reactor Equipment
Electric Furnace
Blacklight (e.g., Magniflux)
Laser
Medical X-ray
Radiography Equipment & Sources
Welding
Electric Arc - Other (High Current Circuits)
Electron Beam
Radar
Alternating Current (AC) Motors

E. Explosive Pyrophoric

Caps
Primer Cord
Dynamite
Power Metallurgy
Dusts
Hydrogen (Inc. Battery Banks and Water Electrolysis)
Gases-Other
Nitrates
Electric Squibs
Peroxides-Superoxides
Propellant

F. Thermal (Except Radiant)

Convection
Heavy Metal Weld Preheat
Exposed Steam Pipes
Electric Heaters
Fire Boxes
Lead Melting Pot
Electrical Wiring & Equipment
Furnaces

G. Flammable Materials

Packing Materials
Rags
Gasoline (Storage & in Vehicles)
Lubrication Oil
Coolant Oil
Paint Solvent
Diesel Fuel
Buildings and Contents
Trailers and Contents
Grease
Hydrogen (Including Battery Banks)
Gases - Other
Spray Paint
Solvent Vats

H. Kinetic-Linear

Cars
Trucks
Buses
Fork Lifts
Carts
Dollies
Trains
Surfaces
Obstructions
Shears
Presses
Crane Loads in Motion
Pressure Vessel Blowdown
Power Assisted Driving Tools
Monorails

I. Mass, Gravity, Height

Human Efforts
Stairs
Lifts
Cranes
Buckets and Ladders
Trucks
Slings
Hoists
Elevators
Jacks
Scaffolds and Ladders
Crane Cabs
Pits
Excavated Doors
Elevated Doors
Canals
Vessels

J. Kinetic-Rotational

Centrifuges
Motors
Pumps
Cooling Tower Fans
Cafeteria Equipment
Laundry Equipment
Gears
Shop Equipment (Grinders, Saws, Brushes, etc.)
Floor Polishers

K. Pressure-Volume/K-Constant-Distance

Test Loops and Facilities
Gas Bottles
Pressure Vessels
Coiled Springs
Stressed Members
Gas Receivers

L. Thermal Radiation

Furnaces
Boilers
Steam Lines
Laboratory and Pilot Plant Equipment
Solar
Boilers
Heated Surge Tanks
Autoclaves

M. Toxic Pathogenic

Acetone
Fluorides
Carbon Monoxide
Lead
Ammonia and Compounds
Asbestos
Trichlorethylene
Dusts and Particulate
Pesticides-Herbicides-Insecticides
Bacteria
Beryllium and Compounds
Chlorine and Compounds
Decontamination Solutions
Sandblasting Operations
Metal Plating
Asphyxiation-Drowning

N. Nuclear

Vaults
Temporary Storage Areas
Receiving Areas
Shipping Areas
Casks
Burial Ground
Storage Racks
Canals in-Tank Storage Areas
Dollies
Trucks
Hand Carry
Cranes
Lifts
Commercial
Shops
Hot Cells
Assembly Areas
Inspection Areas
Test Rigs
Reactors
Critical Facilities
Subcritical Facilities
Laboratories
Pilot Plants

APPENDIX B
PRELIMINARY HAZARD LIST EXAMPLE
GENERAL LABORATORY FACILITY

AREAS OF CONCERN/SAFETY CONSIDERATIONS

(1) Building Materials
- Compatibility
- Flammability
- Structural integrity

(2) Access/Egress
- Emergency - evacuation, fire fighting, rescue
- Panic hardware
- Restricted - security, clean rooms
- Handicapped/disabled
- Operations and maintenance
- Inspection
- Life safety code requirements

(3) Utilities
- Location
- Controls/shutoffs
- Electrical power supply
- Water supply
- Sanitary/sewer
- Natural gas
- Special systems - bulk gas

(4) Ventilation
- Heating
- Air conditioning
- Clean room environment
- Filters/dust control
- Humidity control
- General exhaust
- Emergency
- Recirculation/migration/reentrainment

(5) Electrical
- Emergency power
- Electrostatic discharge

(5) Electrical (Continued)
- Shock
- Wiring
- Switchgear
- Shutoffs/breakers
- Wires/cables under raised floor
- Intra- and inter-room cable management/computer networks
- Grounding/bonding
- Insulation
- Cathodic protection
- Lasers - high energy power supply, capacitors, interlocks
- Lock-out / tag-out

(6) Lighting
- Ambient
- Emergency
- Exit
- Security

(7) Fire Protection
- Fire/smoke detection
- Pull stations
- Alarms/annunciation
- Automatic fire suppression
- Extinguisher selection/location
- Standpipe hose connections
- Siamese connections
- Hydrants
- Smoke management
- Fire resistive construction
- Fire barrier design/construction
- Compartmentalization / isolation from different occupancies
- Fire department access

(8) Monitoring
- System/utility - pressure, temperature, flow, voltage, grounds
- Environmental - air quality, temperature, humidity
- Security
- Fire/smoke detection
- Hazardous gas/vapor detection
- Leak detection
- Alarms/annunciation

(9) Communications
- Public address
- Emergency - fire department, police, medical services
- Alarms/central station

(10) General
- Stairs/railings
- Traffic
- Sidewalks
- Loading/unloading
- Trailer pads
- Height - rooftop observation dome, roof mounted antennae

(11) Natural Phenomena
- High wind
- Snow
- Extreme temperatures
- Floods
- Lightning
- Earthquake

(12) Kinetic/Mechanical
- Sparks/friction
- Overhead cranes
- Machine guards
- Power tools
- Elevators
- Overhead doors
- Staging

(13) Pressure
- Hydraulics
- Compressed gases - bottles, tanks
- Air/pneumatic systems
- Relief valves
- Steam
- Pumps

(14) Confined Space
- Vacuum chambers
- Raised floors
- Utility tunnel

(15) Laboratory Design
- Benches/work surfaces
- Storage
- Drainage
- Exhaust/ventilation
- Clean room environment
- Utilities
- Space utilization/placement
- Cross connection/backflow prevention

(16) Radiation
- Ionizing - alpha particles, beta particles, neutrons, x-rays, gamma rays
- Electromagnetic - lasers, radar, ultraviolet (UV) and infrared (IR) light, microwaves, radio frequency (RF) waves, high frequency signals from computer equipment
- Acoustical - laboratory and ventilation equipment noise
- Thermal

(17) Hazardous Materials
- Flammables/combustibles
- Explosives/pyrophorics
- Toxic substances/poisons
- Corrosives
- Oxidizers
- Water reactive/unstable substances
- Irritants
- Asphyxiants
- Radioactive materials
- Carcinogens/pathogens

(18) Material Handling
- Storage - quantity, location, isolation/fire control areas, compatibility, inventory control
- Transfer/delivery
- Use
- Disposal
- Spill control
- Containment
- Exhaust/ventilation

(19) Environmental
- Resource Conservation and Recovery Act (RCRA) considerations
- Hazardous waste
- Hazardous spill/release

- Exposure to environment
- Exposure from environment

(20) Exhaust
- General
- Local
- Fume hoods
- Emergency
- Scrubber/filtration
- Recirculation/migration/reentrainment

(21) Personnel Safety
- Personal protective equipment - gloves, gowns, eye and ear protection, respirators
- Eyewashes/showers
- Graphics
- Thermal contact - burns (hot and cold)
- Exposure control
- First aid
- Pre-action alarms for carbon dioxide/nitrogen extinguishing systems

(22) Documentation
- Material Safety Data Sheets (MSDS)
- Training
- Emergency action plan
- System safety plan
- Operating procedures
- Maintenance procedures
- Test procedures
- Chemical hygiene plan
- Configuration control plan

(23) Operations
- Electronic/mechanical testing and analysis
- Cooking/kitchen equipment
- Spectroscopy/optics
- Chromatography
- Magnetic analysis
- Cryogenics
- Fabrication/machine shop
- Lasers
- Supercomputer operations

APPENDIX C

EXAMPLE
FACILITY SAFETY MANAGEMENT PLAN
GENERAL LABORATORY FACILITY

TABLE OF CONTENTS

EXAMPLE
FACILITY SAFETY MANAGEMENT PLAN
GENERAL LABORATORY FACILITY

TABLE OF CONTENTS (CONTINUED)